Google North America Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043

February 28, 2018

Via ECFS

Annual 47 CFR § 64.2009(e) CPNI Certification, EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017

1. Date filed: *February 28, 2018*
2. Name of company(s) covered by this certification: *Google North America Inc.*
3. Form 499 Filer ID: *830853*
4. Name of signatory: *John Maletis*
5. Title of signatory: *Chief Operating Officer*
6. Certification:

I, John Maletis, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 CFR § 64.2001 *et seq*.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (i.e., proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 CFR § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed:

Chief Operating Officer, Google North America Inc.

Attachment: Accompanying Statement explaining CPNI procedures

GOOGLE NORTH AMERICA INC. STATEMENT OF COMPLIANCE REGARDING CUSTOMER PROPRIETARY NETWORK INFORMATION ("CPNI")

Google North America Inc. ("GNA" or "Company") provides this statement pursuant to 47 C.F.R. § 64.2009(e) to explain how GNA's operating procedures were designed to ensure compliance with the CPNI rules of the Federal Communications Commission ("Commission") for calendar year 2017.

Safeguarding CPNI

GNA has implemented strong measures to discover and protect against attempts to gain unauthorized access to CPNI. In addition to its internal policies, which are designed to ensure compliance with the Commission's CPNI Rules, GNA publishes an online Privacy Notice for its customers, which explains how GNA uses, discloses, and protects customer information, including CPNI, consistent with applicable law. GNA is committed to constant assessment and improvement in its security and operating procedures with respect to CPNI.

Notice of CPNI Rights and Customer Approval

During the reporting period, GNA did not to use, disclose, or permit access to its customers' CPNI without customer approval except as permitted under 47 C.F.R. § 64.2005, or as otherwise provided in Section 222 of the Communications Act. Accordingly, the customer notice and associated record-keeping requirements of the Commission's CPNI rules (47 CFR §§ 64.2007 and 64.2008) are not applicable. Nonetheless, GNA informed its users through its Privacy Notice that its policies permit disclosure of CPNI only as required or permitted by law, unless the customer opts in to use of CPNI for the purpose of marketing the services of GNA's communications-related affiliates. GNA maintains records of such opt-in approvals for at least one year. Should GNA change its policies such that additional customer notice is required, such notice will be provided.

Marketing Campaigns

GNA has a supervisory review process regarding compliance with the CPNI rules for its outbound marketing campaigns. GNA has dedicated in-house legal counsel responsible for the review of marketing campaigns.

GNA's policy is to maintain, for at least one year, records of sales and marketing campaigns that use CPNI, if any. Records must include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign.

Customer Authentication

GNA has established procedures requiring proper customer authentication prior to disclosing CPNI. For example, GNA's customer support representatives are not authorized to discuss CPNI during customer-initiated telephone contacts unless the customer is first able to provide authentication such as a one-time, randomly-generated password assigned to the customer by GNA. GNA does not have presence in physical retail locations.

Employee & Representative Training Program

GNA provides Company-wide recurring training to educate its employees and representatives regarding the confidentiality of customer information, including authorized and unauthorized uses of CPNI. GNA augments this Company-wide training with targeted training for customer service representatives. Such training provides front-line employees and representatives with additional information concerning safeguarding CPNI and other customer information along with specific training regarding proper authentication of inbound customer inquiries by telephone or online. GNA also provides additional training to other functional groups, such as the marketing and legal departments. All GNA employees are required to certify that they understand their obligations regarding the handling of CPNI.

Employee Discipline Program

Though its parent company, Google LLC, GNA has an disciplinary process in place to address noncompliance with Company policies, including policies concerning employee use of, access to, and disclosure of CPNI. An employee found to have violated GNA's policies, including policies relating to use of, access to, and disclosure of CPNI, is subject to disciplinary action up to and including termination.

Notice of Security Breaches

GNA's policy is to notify law enforcement as soon as practicable, but in no event later than seven (7) business days, after a reasonable determination has been made that a breach of its customer's CPNI has occurred. The notice process conforms to procedures established by the Commission and is otherwise in accordance with 47 C.F.R. § 64.2011.

GNA's policy is to notify customers of the breach no sooner than the eighth business day following completion of the notice to law enforcement unless directed by the U.S. Secret Service or the FBI not to so disclose or notify customers. GNA respects any agency request that GNA not to disclose the breach for an initial period of up to 30 days, which may be extended further by the agency. The requesting agency must provide its direction in writing, as well as any notice that delay is no longer required.

Notice of Opt-Out Failures

GNA's policy is not to use, disclose, or permit access to CPNI without the customer's opt-in approval, or unless permitted or required under the Commission's rules without customer approval. That is, we do not use, disclose, or permit access to CPNI on an opt-out basis. Should this policy change, GNA will provide written notice of any opt out failures to the Commission within five business days as specified in the Commission's rules.

Recordkeeping of Unauthorized Disclosures of CPNI, Customer Complaints, and Actions Taken Against Data Brokers

GNA's policy is to maintain a record of CPNI security breaches, notifications made to law enforcement, and notifications made to customers for at least two years.

GNA's policy is that customer complaints concerning the unauthorized release of CPNI are reported and investigated internally, and are broken out by category of complaint (e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized). A summary of any such complaints during the certification period is included as Attachment A.

A record of actions taken by GNA against data brokers, if any, is maintained and an explanation of such actions is included as Attachment B. GNA did not detect pretexting activities by data brokers during the reporting period. GNA deploys safeguards to protect against, detect, and mitigate pretexting activities.

Remainder of page intentionally left blank

ATTACHMENT A

SUMMARY OF GOOGLE NORTH AMERICA INC.'S CUSTOMER COMPLAINTS CONCERNING THE ALLEGED UNAUTHORIZED ACCESS OR RELEASE OF CPNI

GNA has implemented comprehensive policies and procedures to capture and investigate any customer complaints made to any Company business channel (e.g., customer care, Internet, etc.) concerning alleged unauthorized access or release of CPNI. During the reporting period, GNA did not receive any complaints concerning alleged unauthorized access or release of CPNI.

Complaint Type	**Quantity**
Alleged Unauthorized Access by Employees	0
Alleged Improper Disclosure to Unauthorized Persons	0
Alleged Unauthorized Access to Online Information	0
TOTAL	0

ATTACHMENT B

GOOGLE NORTH AMERICA INC. PROCEEDINGS INSTITUTED OR PETITIONS FILED AGAINST DATA BROKERS

Type of Action	**Quantity**
Court	0
State Commission	0
Federal Communications Commission	0
TOTAL	0